CROSS-LAYERED SECURITY ANALYSIS OF WIRELESS AD HOC NETWORKS

Alvaro A. Cardenas, Nassir Benammar, George Papageorgiou and John S. Baras
Electrical and Computer Engineering Department
and the Institute for Systems Research
University of Maryland
College Park, MD, 20742

ABSTRACT

There is an inherent tradeoff between the performance of a network and its security. In this work we explore possible evaluations of security threats versus the cost of prevention and reaction to such threats. We consider different kind of adversaries with different capabilities. We present the effect of these capabilities on the different layers and the network as a whole. Such a study will help identify the importance of layered security in this infrastructure-less wireless setting.

1. INTRODUCTION

Wireless ad hoc networks are able to provide fast and efficient network deployment capabilities in a wide variety of scenarios where a fixed networking infrastructure is not possible. These types of networks offer new challenging security problems due primarily to their wireless network interface, allowing easy eavesdropping and injection of messages, and to their distributed infrastructure-less topology. The security in wireless ad hoc networks has been analyzed individually at different layers of the communication protocols; however in this summary we provide a novel global assessment of the network by analyzing the risk and vulnerabilities across communication protocol layers under different kind of adversarial settings.

2. SECURITY PROPERTIES

The network assumptions are fundamental for the type of security mechanism we can deploy. Ideally the communication and security properties we want the network to have under any type of adversarial setting are: access control, availability, and end to end message integrity, authenticity, and confidentiality. However, not all of these properties are easily achieved. Some properties even have mutual conflicting goals: providing integrity, authenticity and confidentiality incur in extra computation and bandwidth from the network, which can produce a decrease in network performance, functionality and ultimately, it can affect its availability.

3. ADVERSARY MODEL

In this section we analyze three types of adversarial behavior: Outsiders, adversaries with a single compromised node, and adversaries with *n* compromised nodes chosen selectively. In all cases we study their impact on the desired network properties assuming the adversary acts maliciously at different layers of the communication protocols. Our goal is to identify the key services/layers of the network that pose the greatest security threats when controlled by the adversary.

3.1 Outsiders

Outsiders are attackers that do not have any compromised nodes and hence have no secret key material or trust relationships with other nodes in the network. These adversaries have limited capabilities for disrupting the network services. In particular we note that encrypting at the MAC layer the network traffic with a single key is sufficient to guarantee all of the desired security properties listed in Section 2, except for availability. To interrupt availability of the network, outsiders can attempt to jam the communications channel, they can create a wormhole, and as an extreme attack, we assume they can eliminate nodes from the network.

To prevent jamming, the physical layer should have a large signal to interference ratio. In this area there is a lot of research on spread spectrum technology and codes resilient to malicious interference. On the other side, a wormhole is very difficult to prevent. However, when the MAC layer is encrypted, selecting forwarding by the wormhole can be prevented. That is, the adversary cannot pick which packets to drop and which ones to let through, so the attack has limited impact. As a final attack for outsiders, we also assume the case when they can physically eliminate nodes from the network. The impact

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **00 DEC 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Cross-Layered Security Analysis Of Wireless Ad Hoc Networks**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Electrical and Computer Engineering Department and the Institute for Systems Research University of Maryland College Park, MD, 20742**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**2**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

of this attack depends on the network density and the network connectivity protocols using percolation thresholds (the critical value such that the network is fully connected). This framework can be used to analyze the characteristics that attackers should have (e.g. density in space,) in order to create problems to the network (e.g. break the full connectivity and therefore route availability).

3.2 Insiders

Insiders are adversaries that can compromise nodes or otherwise have a valid identity in a network with appropriate key material. Insiders therefore have the same capabilities as outsiders plus the ability to participate in the network protocols and deviate from the normal behavior of the protocols. Stronger security considerations have to be taken into account for insiders. A minimum level of fault tolerance has to be designed into the network inside attackers. Intrusion detection and response are also among the possible solutions. However the overall network performance degradation, as a result of implementing intrusion detection and response mechanisms has to be compared to the potential network performance degradation due these attackers. An important key issue to consider in the presence of a distributed intrusion detection and response system is the potential of exploitation of such system by malicious nodes. For example, malicious nodes might try to frame good nodes so that they get revoked by other nodes. The goal is then to study which protocols achieve our desired properties despite the active participation of the adversary in the protocol.

In wireless ad hoc networks, the MAC layer is of outmost importance, because it governs the local access, the routing and the flow control. Assuming authentication is provided at each layer, the simplest attempt to degrade the availability of the network with a compromised node is by constantly transmitting over the network. In evaluating these attacks, one needs to consider the cost associated to channel access and the damage that can be done by an outsider with limited battery life. This problem can be leveraged with a MAC layer protocol achieving a certain degree of fairness among contending nodes, or by different channel assignment among each pair of nodes.

The routing layer has been one of the most extensively studied under security considerations. Some possible attacks include route disruption attacks such as routing loops, sink holes (black holes, grey holes, etc.), sub optimal routes, packet dropping, wormholes with selective forwarding, routing rushing attacks etc. It is however less understood the advantages that "secure" routing protocols can provide. It is important to compare the security benefits of proactive (e.g. SEAD) versus reactive (e.g. ARIADNE) protocols and link state routing (e.g. secure OLSR) versus distance vector routing (e.g. SAODV). Some of the routing attacks are launched from the MAC layer. As mentioned above malicious node can alter the traffic flow by launching a denial of service attack on certain nodes or even on all the nodes contained in its transmission range. Therefore, additional interaction between the network and MAC layer would help detect such attacks and slow the performance degradation of the network.

At the highest layers end to end security must be provided. It is however at the application layer where most of the network services run. A dangerous possible exploit in the application layer services are topological worms. As opposed to traditional networks where routers and servers are different, and where routers provide little services, in ad hoc networks each node can act as a server and a router. Furthermore most of the nodes can have the same software, so a single vulnerability would allow an insider to create a stealthy worm that propagates through neighbor lists, compromising incrementally all nodes in the network faster than any detection mechanism can respond to.

CONCLUSIONS

In network security design it is important to provide a global risk assessment of expected performance degradation of the network under different types of adversaries. Due to the limited resources in ad hoc networks, the tradeoff between added security, vulnerability and network performance need to be closely examined and taken into consideration in future efforts. This summary is therefore, the basis of future work to propose cross layer interactions for detecting attacks and to provide intrusion tolerance and graceful degradation designs for network survivability.

ACKNOWLEDGMENTS

Research supported in part by the U.S. Army Research Office under Award No. DAAD19-01-1-0494 to the University of Maryland College Park.